ABSTRACT OF THE DISCLOSURE

[0077] A fast, iterative techique for evaluating M modulo J which may be easily implemented in hardware. In the illustrative embodiment, the invention includes a first circuit (10) for decomposing M into two integers A and B = M – A; a second circuit (20) for evaluating (A modulo J); a third circuit (30) for evaluating M′ = (A modulo J) + B; and, a fourth circuit (40) for determining whether to output M′ as the final answer, or to feedback M′ to said first means to evaluate M′ modulo J.